REMARKS/ARGUMENTS

Favorable reconsideration of this application, as presently amended and in light of the following discussion, is respectfully requested.

Claims 1-6, 8-16, and 18-22 are currently pending, Claims 1, 9, 11, 19, 21, and 22 having been amended. The changes and additions to the claims do not add new matter and are supported by the originally filed specification, for example, on Fig. 5.

In the outstanding Office Action, Claims 9 and 21-22 were objected to for informalities; Claims 1-6, 8-16, and 18-22 were rejected under 35 U.S.C. §112, second paragraph, as being indefinite; Claims 1-5, 9-15, 19, and 20-22 were rejected under 35 U.S.C. §103(a) as being unpatentable over Schneier ("Applied Cryptography," Second Edition) in view of Bo Lin et al. (GB 2345229A, hereafter "Lin"); Claims 6 and 16 were rejected under 35 U.S.C. §103(a) as being unpatentable over Schneier in view of Lin and Kocher et al. (U.S. Pub. No. 2001/0053220A1, hereafter "Kocher"); and Claims 8 and 18 were rejected under 35 U.S.C. §103(a) as being unpatentable over Schneier in view of Lin and Kaminaga et al. (U.S. Pub. No. 2002/0124179A1, hereafter "Kaminaga").

With respect to the objection to Claims 9 and 21-22 for informalities, Applicants respectfully submit that the present amendment to Claims 9 and 21-22 overcome the grounds of objection.

With respect to the rejection of Claims 1-6, 8-16, and 18-22 under 35 U.S.C. §112, second paragraph, the Office Action takes the position that it is unclear how the "input data to be encrypted for a first group of the groups is different relative to the input data to be encrypted for a second group of the groups." Claim 1 has been amended to clarify that "where a first input data to be encrypted for a first group of the groups is different relative to a second input data to be encrypted for a second group of the groups, and the first input data to be encrypted for the first group is generated independently relative to the second input data to be encrypted for the second group." Applicants note that this amendment to Claim 1 corresponds to the examiner's interpretation of the claim described on the bottom of page 6 and the top of page 7 of the Office Action. Additionally, support for this feature is shown on Figs. 5-7, which show in a non-limiting example, that for a first group (X group) there is a first input (A1), and for a second group (Y group) there is a second input (Rc), and the first input (A1) is generated independently of the second input (Rc) (see also page 25, lines 1-17).

Therefore, Applicants respectfully submit that the present amendment to Claim 1, and similarly the amendment to Claims 9, 11, 19, and 21-22, overcomes the ground of rejection under 35 U.S.C. §112, second paragraph.

With respect to the rejection of Claim 1 under 35 U.S.C. §103(a), Applicants respectfully submit that the present amendment to Claim 1 overcomes this ground of rejection. Amended Claim 1 recites, *inter alia*,

> a control section configured to set a mixed encryption processing sequence by dividing an original encryption processing sequence into a plurality of groups, each group being composed of a plurality of encryption processing units, each encryption processing unit being a defined process, each group being a separate and independent encryption process for encrypting an input data, where a first input data to be encrypted for a first group of the groups is different relative to a second input data to be encrypted for a second group of the groups, and the first input data to be encrypted for the first group is generated independently relative to the second input data to be encrypted for the second group, said control section mixing processing sequences of encryption processing units of the plurality of groups with each other by executing performance of at least one encryption processing unit from the first group at a time between executing performance of encryption processing units from the second group and under a condition in which a processing sequence of the encryption processing units within each of the plurality of groups is fixed;
>
> an encryption processing section configured to perform an encryption process in accordance with the

> mixed encryption processing sequence set by said control section; and
>
> a transmitting unit configured to transmit each of encrypted output data generated independently by the first group and the second group to an external device.

Applicants respectfully submit that the combination of Schneier and Lin fails to disclose or suggest all of the features of amended Claim 1.

As previously presented, Schneier is directed to a description of the Data Encryption Standard (DES) and combining block ciphers. In chapter 12, Schneier describes conventional DES, which includes 16 rounds in which a function which uses a key is applied on a plaintext block 16 times (see pages 270-278 of Schneier). In chapter 15, Schneier then describes ways to combine block algorithms to get new algorithms to increase security without designing a new algorithm. In Chapter 15, Schneier describes Double Encryption and Triple Encryption. In Triple Encryption, a ciphertext block is operated on three times with multiple keys (see pages 357-361 of Schneier). Schneier describes different permutations of Triple Encryption based on the types of keys used (see page 360, describing Triple Encryption with Three Keys and Triple Encryption with Minimum Key). Schneier also describes different modes of Triple Encryption involving Cipher Block Chaining (CBC), such as "Inner-CBC" and "Outer-CBC" (see page 360).

As was previously emphasized by the Applicants, in the Triple Encryption described by Schneier, including both Inner-CBC and Outer-CBC modes, ***encryption is being applied to a single plaintext file*** (see page 360, for example, where Schneier describes encrypting "the entire file" for each of the Inner-CBC and Outer-CBC modes). Additionally, a single DES with 16 rounds still has just one independently generated input (the initial input), because any subsequent input into any of the later rounds is derived from an input from the previous round. Thus, any one of these processes being described in Schneier constitutes only a single group as defined by Claim 1 because each of the processes described in Schneier is still just directed to a single independently generated input being put through an overall encryption process to produce a single encrypted output.

The Office Action also appears to acknowledge this point in indicating that "Schneier does not explicitly disclose the input data is different for a first group and second group; the input data to be encrypted for the first group is generated independently relative to the input data to be encrypted for the second group." (See Office Action, at page 10).

The Office Action relies on Lin to remedy this deficiency of Schneier.

Lin describes inserting "dummy" S-block lookups into a real DES process (see page 11, lines 10-13). The Office Action relies on such a dummy S-block lookup as corresponding to the claimed "second group" which has an independently generated input from a "first group." (See Office Action, at page 10). However, Lin explicitly describes the following on page 11, lines 10-15:

> Another technique which could be used to improve resistance to attacks is to insert a "dummy" operation to confuse analysis of a power signature. For example, one could insert "dummy S block look-ups into the DES routing, **whereby an S block look-up is performed but the result or output of the look-up is not included in the pre-output value, U, but is instead written elsewhere and not used**. [Emphasis added].

On the contrary, amended Claim 1 defines "a transmitting unit configured to transmit each of encrypted output data generated independently by the first group and the second group to an external device." In other words, in Claim 1 both the "first group" and "second group" are "separate and independent encryption process for encrypting an input data" and since the output of first group and second group are both transmitted to an external device they both have output values ***that are used***.

Therefore, each of the "first group" and "second group" of Claim 1 is explicitly different than a dummy S-block lookup described in Lin. Thus, the dummy S-block of Lin cannot be interpreted to correspond to the "second group" as defined by amended Claim 1, and therefore inserting the dummy S-block lookups of Lin into a process of Schneier as asserted in the Office Action would not achieve all of the features of amended Claim 1.

Therefore, Applicants submit that Lin clearly fails to remedy the deficiencies of Schneier with regard to amended Claim 1.

Accordingly, the combination of Schneier and Lin fails to disclose or suggest all of "a control section configured to set a mixed encryption processing sequence by dividing an original encryption processing sequence into a plurality of groups, each group being composed of a plurality of encryption processing units, each encryption processing unit being a defined process, ***each group being a separate and independent encryption process for encrypting an input data, where a first input data to be encrypted for a first group of the groups is different relative to a second input data to be encrypted for a second group of the groups, and the first input data to be encrypted for the first group is generated independently relative to the second input data to be encrypted for the second group...a transmitting unit configured to transmit each of encrypted output data generated independently by the first group and the second group to an external device***."

Therefore, Applicants submit that amended Claim 1 (and all associated dependent claims) patentably distinguishes over Schneier and Lin, either alone or in proper combination.

Kocher and Kaminaga have been considered but fail to remedy the deficiencies of Schneier and Lin with regard to Claim 1. Thus, Applicants respectfully submit that amended Claim 1 (and all associated dependent claims) patentably distinguishes over Schneier, Lin, Kocher, and Kaminaga, either alone or in proper combination.

Independent Claims 9, 11, 19, 21, and 22 recite features similar to those of amended Claim 1. Thus, Applicants respectfully submit that Claims 9, 11, 19, 21, and 22 (and all associated dependent claims) patentably distinguish over Schneier, Lin, Kocher, and Kaminaga, either alone or in proper combination.

Consequently, in light of the above discussion and in view of the present amendment, the outstanding grounds for rejection are believed to have been overcome. The present application is believed to be in condition for formal allowance. An early and favorable action to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Bradley D. Lytle
Attorney of Record
Registration No. 40,073

Sameer Gokhale
Registration No. 62,618

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413-2220
(OSMMN 08/07)